Appln. No. 10/535,755
Reply to Office Action of June 23, 2008

VIA EFS

Amendments to the Drawings:

The attached sheet of drawings includes changes to Figure 1. This sheet replaces the original sheet including Figure 1. In Figure 1, structures 10 and 20 have been identified as random number generator 10 and bit register 20. Support for these changes may be found at paragraphs [0030]-[0034] and [0038] of the Specification. Structures 2 (CPU) and 8 (memory) have been added. Support for the addition of these structures may be found at paragraph [0003] of the Specification.

Attachments: Replacement Sheet
              Annotated Sheet Showing Changes

Appln. No. 10/535,755
Reply to Office Action of June 23, 2008

VIA EFS

REMARKS

A. GENERALLY

  Claims 1-14 remain in the Application. Claims 1 and 10 have been amended. Claims 11-14 have been added. No new matter has been added.

B. CLAIM OBJECTIONS

  Claim 10 has been objected to as being an improper multiple dependent claim. Claim 10 has been amended to depend solely from claim 1. Applicant submits that claim 10 as currently listed is in proper form and requests that the objection to this claim be withdrawn.

C. CLAIMS REJECTIONS

1. Claim Rejections Pursuant to 35 U.S.C. § 102

  Claims 1-10 have been rejected under 35 U.S.C. 102(a) as being anticipated by U.S Patent 6,327,661 issued to Kocher et al. (hereinafter, "Kocher").

Claim 1 recites the following limitations:

> 1. A microcontroller the programming of which is carried out in at least one machine-dependent assembler language in which the assembler commands, with the exception of conditional program jumps or program branches, respectively, can be executed in essence independently of data,
>
> characterized by at least one random number generator assigned to the microcontroller,
>
> by means of which the program jumps or program branches can be executed in dependence on the state of the random number generator
>
> and/or independently of the internal state of the programming of the microcontroller.

  The Office Action asserts that the disclosure at Col. 7, lines 20-25 and Figure 2 of Kocher teaches these limitations:

> Referring now to FIG. 2, random number generator 200 (which can be, but need not be, implemented in hardware) is used to determine which clock cycles (or clock state transitions) are to be used by microprocessor core 225. Random number generator 200 produces a stream of random (or pseudorandom) digital output bits or analog noise as random output 205.

  Kocher describes techniques for inhibiting the external observation of a microcontroller's internal operation by techniques that increase the noise (uncorrelated data) over data that can be correlated. For example, one technique uses a random number to determine which clock cycles (or clock state transitions) are to be used by the microprocessor core. Alternatively, the random output can be used to select the closest corresponding cycles of clock signal to be used as the

processor clock signal. According to Kocher, "the basic point being that clock signal 260 be (partially or wholly) decorrelated from external clock signal 220 via random output 205."

The Office Action asserts that the limitation, "means of which the program jumps or program branches can be executed in dependence on the state of the random number generator" is met because "(...Kocher teaches random number generation [fig. 2] used to determine clock cycles [col.7, lines 20-25])." (Office Action, p. 4, ¶6.)

Applicant respectfully submits that the use of random number generation to determine clock cycles does not teach or reasonably suggest the execution of program jumps or program branches in dependence on the state of the random number generator as recited in claim 1. The operation of claim 1 is not dependent on an external clock as described in Kocher but on the use of a random number to execute jumps or branches within an instruction set to obscure the operation of the microcontroller.

Claims 2-4 and claim 10 (as amended) depend from claim 1 and recite all of the limitations of that base claim. Based on the foregoing, claims 2-4 and 10 recite limitations not taught or reasonably suggested by Kocher and are not anticipated by that reference.

Claim 5 recites the limitations:

> 5. A method for processing the programming of a microcontroller executed in at least one machine-dependent assembler language, the assembler commands, with the exception of conditional program jumps or branches, being executed essentially independently of data, characterized in that the program jumps or program branches are executed in dependence on the state of at least one random number generator and/or independently of the internal state of the programming of the microcontroller.

Claim 5 has been rejected on the same grounds a claim 1. For the reasons set forth in the discussion of claim 1, claim 5 recites limitations not taught or reasonably suggested by Kocher and is not anticipated by that reference.

Claims 6-9 depend directly or indirectly from claim 5 and recite all of the limitations of that base claim. Based on the foregoing, claims 6-10 recite limitations not taught or reasonably suggested by Kocher and are not anticipated by that reference
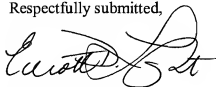
D.   NEW CLAIMS 11-14

Claims 11-14 have been added to the present application. Support for the newly added claims may at least be found at paragraphs [0013]-[0016].

E.   CONCLUSION

Applicant respectfully submits that the claims as currently listed are in condition for allowance. Applicant requests that this response be entered and that the current rejections of the claims now pending in this application be withdrawn in view of the above amendments, remarks and arguments.

Respectfully submitted,

Elliott D. Light, J.D.
Registration No. 51,948
Jon L. Roberts, Ph.D., J.D.
Registration No. 31,293
Roberts Mardula & Wertheim, LLC
11800 Sunrise Valley Drive, Suite 1000
Reston, VA 20191-5302
(703) 391-2900

ATTACHMENTS:

1.   Replacement Sheets for Figure 1

2.   Annotated Sheet Showing Changes in Figure 1